Official Call for Proposals

Issued by the Digital Transmission Discussion Group Copy Protection Technical Working Group Version 1.0

Scott Smyers
Sony US Research Laboratories
3300 Zanker Road
M/S SJ3D3
San Jose, CA 95134
Chairman, Digital Transmission Discussion Group

March 11, 1997

"OUTSIDE COUNSEL'S EYES ONLY"

1. Purpose

1.1 Overview

The Digital Transmission Discussion Group (DTDG), which is a sub-group of the Copy Protection Technical Working Group (CPTWG), is hereby issuing this Call for Proposals ("CFP") for a data protection system ("DPS") that can be used to protect, at a minimum, digital video or digital audio transmitted on the IEEE 1394-1995 High Performance Serial Bus using the isochronous data transport mechanism. The purpose of the DPS is to prevent the casual copying, by consumers, of copy protected information. This CFP specifies the requirements for the DPS.

1.2 The Data Protection System

The DTDG intends to develop, and to recommend to the CPTWG, a DPS that is comprised of one or more of three layers:

1) Copy Control Information - CCI

2) Data encryption

3) Authentication

This CFP requests proposals for any one, two or three of these layers. Proposals may address a single layer, or multiple layers in combination.

Proposals must address the issue of key exchange, if such is required for the proper operation of the proposed DPS. The DTDG does not make any recommendations on how key exchange plays a part in the proposed DPS, nor in which of the three layers listed above the key exchange protocol should reside.

1.3 Requirements for DPS

This section describes required characteristics of the target DPS.

1.3.1 General Requirements

The members of the CPTWG require a means by which content sent through digital transmissions can be kept secure from unauthorized access or copying and that devices can be manufactured to implement, and comply with the specifications for, the DPS. In order to enforce adherence to the requirements of the DPS, the target DPS that the DTDG will ultimately recommend, whether making use of only one layer, or multiple layers in combination, will make use of intellectual property, and the intellectual property relating to the DPS shall be licensed to device manufacturers such that products not conforming to the DPS would constitute a breach of the license. It is not necessary that every proposal contain intellectual property, but proposers should recognize that the DTDG will consider proposals which do not contain intellectual property as only a part of the final DPS, and not as a complete DPS.

It is a condition of submitting a proposal in response to this CFP that, if such proposal is selected by the CPTWG and the person submitting the proposal owns intellectual property relating to the proposed DPS, then such person must be prepared to license such intellectual property on fair, reasonable and non-discriminatory terms. Any such person shall cooperate in good faith with potential licensees to make such a license available, whether directly to licensees or indirectly, through a licensing entity.

The members of the CPTWG recognize that where there is a will to circumvent the DPS, a way will be found to do so, regardless of the theoretical strength or complexity of the system. To enforce the requirements of the DPS against both licensees of the DPS who manufacture products that are not in conformity with the specifications for the DPS and all persons who are, without authorization, bypassing, decrypting or otherwise circumventing the system, the members of the CPTWG intend to seek appropriate federal anti-circumvention legislation that would prohibit such bypass, decryption or other circumvention activities.

1.3.2 Technical Requirements

At a minimum, the DPS is required to protect isochronous data transmissions between devices interconnected using the IEEE 1394-1995 High Performance Serial Bus. In this environment, isochronous data transmissions are multi-cast by definition, and therefore, any interconnected device can dynamically begin listening to or cease listening to a source of isochronous data at any time. When a new device begins listening to or ceases listening to a stream which is protected by the DPS, there must be no user perceptible consequences for any existing transmissions between interconnected devices. There is no requirement to protect IEEE 1394-1995 asynchronous transmissions among interconnected devices.

The DTDG requires that the DPS protect copy protected information when it is transmitted among single function consumer devices and general purpose devices such as personal computers interconnected with the IEEE 1394-1995 High Performance Serial Bus. It is the expressed intention of the DTDG that the final DPS will be implemented in all devices which are capable of handling copy protected information, including personal computers and consumer devices.

The DTDG recognizes that the behavior of some devices, such as single function consumer devices, can not be modified by the consumer. Additionally, the DTDG recognizes that the behavior of other devices, such as personal computers, can be altered by the consumer through such means as user loadable software or user installable hardware. Therefore, the DTDG recognizes that it may (or may not) be required to recommend to the CPTWG, additional technologies to complement the DPS in such a way that the security of the copy protected information is maintained after it is received by a general purpose device, such as a personal computer, and is exchanged inside such a device among various software and hardware elements from different vendors.

1.4 Responses

All proposals shall be received by Scott Smyers, the chairman of the DTDG, at the address appearing on the first page of this CFP by 5:00 p.m. (PST) April 25, 1997. Persons submitting proposals must submit ten hard copies and one electronic copy in Microsoft Word or PDF format on a standard IBM formatted 1.44MB floppy disc. Late responses will not be considered.

Prior to the deadline for receipt of proposals, any questions regarding this CFP must be submitted in writing by April 1, 1997, to Scott Smyers.

2. Copy Control Information (CCI) Layer

2.1 Requirements

2.1.1 Carriage of CCI

The DTDG requests proposals which define how to carry CCI in, or strongly associated with, a stream of copy protected data.

Appendix A of this CFP restates the definition of Copy Control Information bits currently adopted for use in applications requiring copy control. Proposers should recognize that the DTDG intends for the CCI layer of the DPS to be used for technologies other than those explicitly mentioned in Appendix A.

At a minimum, proposals for the CCI layer should define a means of carrying the following CCI from a source of a stream of copy protected data to a destination:

1) CGMS

2) APS

3) Digital Source Bit

The DTDG will not reject proposals which permit more CCI information to be carried, nor will the DTDG reject proposals which carry less CCI.

It should be understood that even if the CCI layer adopted by the DTDG for recommendation to the CPTWG carries all three types of CCI information listed above, the CPTWG may still require additional CCI to be carried, such as SCMS Category Bits. The DTDG will make efforts to assure that the CCI layer it recommends to the CPTWG meets all anticipated requirements.

2.2 Descriptions

2.2.1 Frequency

The proposal must describe in detail the frequency or granularity with which the CCI will appear in the content stream (e.g., in each frame, in each isochronous packet, every second, etc.). It is not a requirement that every isochronous packet contain all of the CCI.

Proposals which carry CCI more frequently and/or which explicitly identify a greater amount of information as being copy controlled will be viewed more favorably than proposals which permit more information to be transmitted which is not labeled as copy controlled.

2.2.2 Hardware and Software Implementation

The proposal must provide, at a minimum, sufficient information for an average engineer skilled in the art to construct a means of generating and detecting the CCI in hardware and/or software.

3. Encryption/Decryption Layer

The DTDG requests proposals that describe a method of both encryption (or scrambling) and decryption (or descrambling) of a continuous stream of digital video or digital audio data (the "encryption algorithm"), including any details of keys used in the algorithm, if applicable.

3.1 Requirements

3.1.1 Protection on IEEE 1394 Bus

The encryption algorithm must protect an isochronous channel transmitted on the IEEE 1394-1995 High Performance Serial Bus, consistent with the requirements stated in Section 1.3, "Requirements for DPS". It is acceptable if the encryption algorithm can only be used on the IEEE 1394-1995 interface. However, it is not necessary for the encryption algorithm to rely on features of IEEE 1394-1995, nor on the features of any other digital transmission interface.

3.1.2 Implementation Requirements

It must be possible to implement the encryption algorithm in hardware and/or software, within the general guidelines described in Section 3.1.4. Furthermore, it must be reasonable to implement the encryption algorithm in small, low cost consumer electronics devices and in personal computers.

3.1.3 Export/Import

It should be possible to import the encryption algorithm into and export the encryption algorithm from the maximum number of countries, including but not limited to the United States, France and other member countries of the European Community (EC) and Japan.

3.1.4 Simplicity

Consistent with the objective of protecting copy protected digital transmissions, one requirement of the DTDG is that it should be relatively simple to implement the encryption algorithm. The DTDG has formulated rough benchmarks against which the relative simplicity of all proposals will be evaluated:

1) In order to implement the encryption algorithm in hardware at either the transmitter or the receiver, the proposed encryption algorithm should require approximately 10% or less of the digital logic necessary to implement the 1394 link core, which includes the functionality of the link layer as defined in the IEEE 1394-1995 standard. (Based on public knowledge of existing implementations, the link core can be implemented in approximately 10,000 gates of digital logic).

2) In order to implement the encryption algorithm in software at either the transmitter or receiver, the proposed encryption algorithm should require approximately 3% or less of the processing power that is required to produce a baseband digital video stream from an MPEG-2 compressed digital stream.

3.1.5 Performance

The encryption algorithm, as implemented within the constraints of the simplicity requirement described in Section 3.1.4, shall be capable of handling a stream of MPEG-2 data at a minimum transmission rate of 25 Mbps.

Proposals will be evaluated more favorably if the encryption algorithm can also handle higher bandwidth streams, such as higher bandwidth MPEG-2 rates, or streams of different formats, such as Standard Definition (approximately 30Mbps) and High Definition (approximately 60Mbps) digital video rates, as defined in the Digital Video Consortium "Blue Book".

3.1.6 Strength

Given the importance of protecting copy protected data, the encryption algorithm should be robust. Circumvention of the encryption algorithm should be as difficult as possible.

3.1.7 Resistance to Product Obsolescence

Products implementing the encryption algorithm must not become obsolete between the time that they are introduced in the market and the time that they may otherwise become obsolete due to market influences not related to copy protection.

(For example, if the proposal provides a means to change the encryption algorithm, and if, in fact, the algorithm is changed in the future, then existing devices must be able to transmit to, and receive and play digital content from, devices complying with the requirements of the changed encryption algorithm, and future devices, complying with the requirements of the changed encryption algorithm, must be able to transmit to, and receive and play digital content from, older devices.)

3.2 Descriptions

3.2.1 Simplicity and Performance

To the extent feasible, the proposal should provide an estimate of the complexity to implement the encryption algorithm in hardware, expressed in terms of an approximate number of gates or some other appropriate metric. The proposal should also provide an estimate of the complexity to implement the encryption algorithm in software, expressed as some fraction of the amount of processing power needed to decompress a stream of MPEG2 data of some description, or some other appropriate metric. For encryption algorithms that can handle higher bandwidth streams, the additional complexity of the proposal, if any, necessary to handle higher bandwidth streams should be described.

3.2.2 Robustness

The proposal must contain an assessment of the relative difficulty of unauthorized decryption of the encrypted content and of the ease with which the average consumer can make use of unauthorized decryption hardware or software to circumvent the DPS.

If pcssible, the encryption algorithm should be such that detailed knowledge of a given implementation of this algorithm should not, in and of itself, be sufficient information to allow the production of circumvention devices.

3.2.3 Obsolescence

The proposal must describe the extent to which products that implement the encryption algorithm will be resistant to obsolescence.

4. Authentication Layer

The DTDG requests proposals that describe method by which various elements of a system can mutually determine their authenticity as compliant, trusted devices (the "authentication method").

4.1 Requirements

4.1.1 Authentication on IEEE 1394 Bus

The authentication method must operate such that two devices connected via the IEEE 1394-1995 High Performance Serial Bus can mutually determine their authenticity. It is acceptable if the authentication method can only be used on the IEEE 1394-1995 interface. However, it is not necessary for the authentication method to rely on features of IEEE 1394-1995, nor on the features of any other digital transmission interface.

4.1.2 Hardware and Software Implementation

It must be possible to implement the authentication method in either hardware, software, or some combination, within the general guidelines and environments described in Section 4.1.4.

4.1.3 Export/Import

This requirement, for the authentication method, is identical to the corresponding requirement described in Section 3.1.3.

4.1.4 Simplicity

Consistent with the objective of protecting copy protected digital transmissions, one requirement of the DTDG is that it should be relatively simple to implement the authentication method in any device or piece of software.

In particular, it should be noted that many consumer electronics devices implement the consumer electronics protocols for IEEE 1394 using a simple micro-controller, such as an 8 or 16 bit micro-controller with 64KBytes or less of embedded ROM and 2KBytes total of available RAM. Accordingly, the resources necessary to implement authentication in a consumer electronics device must be well within the limits of such a micro-controller.

In addition, the authentication method must be easily adapted to the PC environment, where typically, most responsibility for implementing various protocols is placed on a single Central Processing Unit (CPU). Therefore, implementing the authentication method in a Personal Computer should not require the addition of special purpose hardware dedicated solely to this purpose.

4.1.5 Performance

A device implementing the authentication method must not behave perceptibly different, from the standpoint of the user experience in all operations, than an identical device not implementing the authentication method.

For example, if implemented on a consumer electronics device that uses a simple micro-controller, then the additional burden of performing the authentication method with another such device using a similar micro-controller should not noticeably affect the user experience, even if the same micro-controller has other responsibilities, such as servo/motor control, etc.

4.1.6 Strength

Given the importance of protecting copy protected data, the authentication algorithm should be robust. Circumvention of the authentication algorithm should be as difficult as possible.

4.1.7 Resistance to Product Obsolescence

Products implementing the authentication method must not become obsolete between the time that they are introduced in the market and the time that they may otherwise become obsolete due to market influences not related to copy protection.

(For example, if the proposal provides a means to change the authentication method, and if, in fact, the authentication method is changed in the future, then existing devices must be able to transmit to, and receive and play digital content from, devices complying with the requirements of the changed authentication method, and future devices, which comply with the requirements of the changed authentication method, must be able to transmit to, and receive and play digital content from, older devices.)

4.2 Descriptions

4.2.1 Simplicity and Performance

To the extent feasible, proposals should estimate the complexity to implement the authentication method. To this end, proposals may specify a target microprocessor and clock rate, specify the amount of RAM and ROM required, and describe approximately how much time would be required for two such devices to complete the authentication method. If special hardware is necessary or useful for implementing the authentication method, then the proposal should also describe such hardware.

The proposer is free to employ some means other than that described in the preceding paragraph to describe the simplicity and performance of the authentication method.

4.2.2 Robustness

The proposal must contain an assessment of the relative difficulty of compromising the security of the authentication method.

If possible, the authentication method should be such that detailed knowledge of a given implementation of this method should not, in and of itself, be sufficient information to allow the production of circumvention devices.

4.2.3 Obsolescence

The proposal must describe the extent to which products that implement the authentication algorithm will be resistant to obsolescence.

5. Evaluation Criteria

The DTDG will evaluate and compare all proposals submitted on the basis of the stated requirements (including the requirement, stated in Section 0.3, that proposed technologies, either alone or in combination with others, contain licensable intellectual property), the information requested above and the criteria described in the subsections below, among others.

The evaluation criteria described in the sections below are not ranked in order of priority. The DTDG may, at its discretion, choose to accord more relative weight to one or more of the criteria, or use other criteria.

After reviewing the proposals submitted, the DTDG will report and make a recommendation to the CPTWG for its consideration.

5.1 Implementation Methods

All proposals will be considered on their amenability to implementation in consumer electronic devices and personal computers. This criterion will require careful evaluation of possible implementation methods, such as special purpose hardware, complex software or possible combinations of the two.

5.2 Importability/Exportability

Proposals for technology that can be exported from, or imported into, the greatest number of countries, including but not limited to the United States, France and other member countries of the European Community (EC) and Japan, will be rated more favorably.

With respect to the United States, although U.S. law is undergoing revision at this time, for purposes of this criterion, the DTDG will apply U.S. law effective as of the date of selection.

5.3 Simplicity

Proposals that are simpler, as evaluated in light of the simplicity benchmarks and other criteria set out above, will be evaluated more favorably than proposals that are more complex and require greater amounts of hardware or software processing.

5.4 Robustness

Proposals that are more robust to unauthorized decryption, circumvention or bypass will be evaluated more favorably.

5.5 Resistance to Product Obsolescence

Proposals that are more resistant to the problem of devices in the field becoming obsolete will be evaluated more favorably.

6. Conditions Relating to the Submission of Proposals

6.1 General Conditions

Given the possibility that the DPS may be comprised of one or more layers, persons submitting proposals should understand that the DTDG may recommend, and the CPTWG may select, a combination of technologies from among different sets of proposals. Therefore, persons making submissions should be prepared for the possibility that, if their proposals are selected, they may be required to license their proposed technologies in conjunction or in combination with technologies proposed by others.

During the process of evaluating the proposals, the DTDG and the CPTWG reserve the right to ask to meet with persons submitting proposals, or may request that additional information or other materials be submitted. Persons submitting proposals shall bear all costs that they incur relating to the preparation, submission and evaluation of such proposals, or that they incur during the process of negotiating any rights to use the technology proposed.

The submission by any person of a proposal in response to this CFP constitutes agreement by such person with all of the terms and conditions set out herein should such proposal be selected by the CPTWG.

THIS CFP DOES NOT CONSTITUTE AN OFFER BY THE DTDG OR THE CPTWG AS TO WHICH THE SUBMISSION OF PROPOSALS WOULD BE REGARDED AS AN ACCEPTANCE. THE DTDG AND THE CPTWG SHALL, IN NO CIRCUMSTANCE, HAVE ANY OBLIGATION TO ANY THIRD PARTY BASED ON THIS CFP, OR ON ANY PROPOSAL SUBMITTED IN RESPONSE THERETO.

ALTHOUGH THE DTDG INTENDS TO MAKE A RECOMMENDATION TO THE CPTWG, ALL PERSONS SUBMITTING PROPOSALS SHOULD BE AWARE THAT THE DTDG MAY RECOMMEND NONE OF THE PROPOSALS TO THE CPTWG. IN ADDITION, THE CPTWG MAY DECIDE NOT TO SELECT ANY PROPOSALS AT THIS OR ANY LATER TIME AND THE CPTWG MAY, SOLELY AT ITS DISCRETION, DECIDE NOT TO PROCEED WITH THE DEVELOPMENT OF A DPS. THE CPTWG MAY SELECT A PROPOSAL, IF ANY, ON THE BASIS OF ANY OF THE CRITERIA SET OUT IN THIS CFP OR OTHERWISE.

6.2 Confidentiality of Proposals

It is understood that valuable and proprietary confidential information may be critical to any technology that is being proposed for any one of the three layers.

NONETHELESS, PROPOSALS SHOULD NOT CONTAIN INFORMATION WHICH IS COMPANY PROPRIETARY OR CONFIDENTIAL. THOSE SUBMITTING PROPOSALS ACKNOWLEDGE THAT MEMBERSHIP OF THE DTDG IS NOT RESTRICTED, AND THAT REPRESENTATIVES FROM DIRECT COMPETITORS WILL HAVE ACCESS TO ALL PROPOSALS. PERSONS SUBMITTING PROPOSALS EXPRESSLY ACKNOWLEDGE THAT ANY AND ALL INFORMATION CONTAINED IN THAT PROPOSAL WILL NOT BE TREATED AS CONFIDENTIAL AND SHOULD NOT BE MARKED AS SUCH.

Accordingly, persons submitting information should use their own judgment to describe generally, but sufficient to permit evaluation by the DTDG and the CPTWG, the technologies they are proposing.

At such time as the DTDG or the CPTWG believe appropriate, whether before or after selection of a proposal or proposals (if any), any person submitting a proposal may be requested to enter into one or more non-disclosure agreements with respect to such technologies for purposes of further, detailed evaluation by the DTDG or the CPTWG.

Appendix A - Copy Control Information

This Appendix defines the bits which convey Copy Control Information, as referenced in Section 1 of the Call for Proposals. Four types of information, comprising 5 bits, are defined below:

1. Copy Generation Management Information

Two bits of data are used to indicate whether and to what extent copying of the material so encoded may be copied, according to the following settings:

1) 0,0 - Copying is permitted without restriction

2) 0,1 - Condition not to be used

3) 1,0 - One generation of copies may be made

4) 1,1 - No digital copying is permitted

These data may be used to indicate, for example, the settings of copy and generation management information encoded using CGMS system for digital and analog video signals, and using the SCMS system for digital audio.

2. Analog Protection System ("APS") Trigger Bits

Two bits shall be provided in digital signals so as to trigger the APS system in analog signals constituting a motion picture. The trigger bits will permit a copyright owner to trigger independently the two different elements of the APS: a "pseudo-sync pulse" ("PSP") element; and an inverted split color burst element which can be employed in two-line and four-line implementations. The settings of these bits are as follows:

APS Trigger	APS Result
0,0	Off
0,1	PSP on; Inverted split color burst off
1,0	PSP on; 2-line inverted split color burst on
1,1	PSP on; 4-line inverted split color burst on

3. Digital Source Bit

A single bit is used to indicate whether the source of the data is a prerecorded ROM disc that has been encoded by the copyright owner with Copy Generation Management Information bits set as "1,1". The settings for the Digital Source Bit are as follows:

1) 0 - Not a prerecorded DVD-ROM disc encoded with CGMS as "1,1"

2) 1 - Prerecorded DVD-ROM disc encoded by the copyright owner with CGMS as "1,1"

7. Appendix B: DTDG Call for Proposals

8. Appendix C: DTDG Request for Supplemental Evaluation Data

9. Appendix D: Final Draft of all Proposals